(21)

Office of the Comptroller of the Currency
Public Information Room
250 E Street, SW
Mail Stop 1-5
Washington, D.C. 20219
Attn: Docket No. 03-18
regs.comments@occ.treas.gov

Board of Governors of the Federal Reserve System
c/o Ms. Jennifer J. Johnson, Secretary
20th Street and Constitution Ave., NW
Washington, D.C. 20551
Attn: Docket No. OP-1155
regs.comments@federalreserve.gov

Federal Deposit Insurance Corporation
c/o Mr. Robert E. Feldman, Executive Secretary
550 17th Street, NW
Washington, D.C. 20429
Attn: Comments/OES
comments@fdic.gov

Office of Thrift Supervision
Regulation Comments, Chief Counsel's Office
1700 G Street NW
Washington, D.C. 20552
Attn: No. 03-35 regs.comments@ots.treas.gov

October 14, 2003

Re: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

Greetings:

(1) Microsoft Corporation submits the following comments in response to the request for comments regarding the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("Guidance").[1] Responding to the invitation to suggest clarifications or to comment on components of the Guidance, we have framed our comments to provide a response that we hope will be informative and responsive.

Microsoft Corporation

(2) In limited circumstances Microsoft could be viewed as a "financial institution" under the Gramm-Leach-Bliley Act (GLB)[2] because of the broad definition in that act. Concepts applicable to true financial institutions do not necessarily translate well for the broader group of "financial institutions" covered by GLB, yet that broader group can be impacted by actions taken by regulators for true financial institutions.[3] Accordingly, we respectfully provide the following comments for your consideration.

Comments

(3) **Part II,B, Suspicious Activity Reports**. The disparity between the GLB definition of "financial institution" and definitions in other statutes can have unintended consequences for companies like Microsoft who are not "real" financial institutions. For example, Part II, B of the Guidance requires[4] a GLB financial institution to file a Suspicious Activity Report (SAR). Absent the immunity provided by

[1] 68 F.R. 47954(2003), Part II.
[2] 15 USC 6809(3)(A).
[3] See 15 USC §§ 6801(b), 6804(a)(2)(requiring FTC to issue consistent regulations).
[4] Although termed "guidance," footnote 5 of the Guidance states that regulators may treat an institution's failure to implement the Guidance as a violation of GLB. 68 FR 47954 at 47956, Note 5. Whether GLB requires an actual rule, as opposed to guidance, is beyond the scope these comments.

the SARs statute,[5] entities who file SARs can be sued for invasion of privacy, defamation and the like, so immunity is critical to anyone required or encouraged to file a SAR. However, the immunity only applies to financial institutions as defined in the SARs statute, a definition that does not cover all GLB financial institutions.[6] The Secretary of the Treasury is authorized to expand SARs coverage but only by regulation. Even if expansion were advisable (which, for other reasons, is not a given), the Guidance is not a regulation. Accordingly, the Guidance should make it clear that entities not clearly immune under 31 USC § 5318(g)(3) need not file a SAR. Of course, this will not be an issue if the FTC issues guidance not containing the SARs requirement, but given the obligations of it and the other agencies to issue "consistent" regulations, it seems prudent to highlight the problem.

(4) **Part II,D,1, Flagging Accounts; Forced Breach of Contract.** The Guidance requires financial institutions to "implement controls to prevent the unauthorized withdrawal or transfer of funds from customer accounts" after an appropriate incident. Understandably, this requirement reflects the orientation of regulators for "real" financial institutions, but may need clarification for financial institutions which do not handle funds or whose activities are not confined to handling funds. Is the requirement simply inapplicable to those institutions or activities or must analogous action be taken? For example, if financial institution #1 processes data containing customer information of financial institution #2, must #1 bar access to the database or withdrawal of information from it after an incident? If the answer is yes, that should be clarified.

(5) If the answer to the above question is yes, the denial of service required by the Guidance may cause a breach of contract. For example, before issuance of the Guidance financial institution #1 may have contracted with #2 to provide 24 hour access to the database for a set term such as 3 years. Must #1 breach its contract in order to comply with any Guidance requirement (if any) regarding denial of access, or with other requirements in the Guidance impacting contracts such as the requirement to change access codes and to impose additional controls on service providers? Some contracts allow suspension of access when required by "law or regulation," but the Guidance is neither. Some contracts allow amendment to impose further duties or controls. But most do not: the subject matter of the Guidance is a new and unusual threat with dimensions that are only beginning to be identified or understood, let alone memorialized in contracts that would allow financial institutions to comply with the Guidance without breach of contract. This is especially true for GLB financial institutions who are not "real" financial institutions and, thus, have not previously encountered a regulatory regime effectively requiring particular kinds of contracts. The Guidance should make it clear that breach of contract is not required for compliance with the Guidance and that institutions are not required to obtain amendments to existing contracts. Reasonable counter-parties will not agree to "ensure" for the financial institution something that cannot be ensured, nor should it be assumed that they will take on increased risks without a commensurate price increase.

(6) In addition to questions concerning forced breach or amendment of contract, is the question of whether the containment and control mechanisms contemplated by the Guidance exceed what is reasonable. Assume a reasonable investigation indicating that further unauthorized access *might* occur because of an incident, but denial of service to customers is *certain* to occur if all of the measures required by the Guidance are taken to "ensure" against unauthorized access (e.g., shutting down applications and third party connections, reconfiguring firewalls, changing customer access codes and the like). The Guidance says these actions will depend upon "the facts and circumstances,"[7] but an institution concerned about a hindsight judgment by its regulator or litigation, may feel compelled to treat every situation as a need to secure Fort Knox. Again, that is impossible in an economy where even the

[5] See 31 USC § 5318(g)(3).
[6] See 31 USC § 5312(a)(2).
[7] Part I,C.

government cannot "ensure" that an electronic (or non-electronic) "Fort Knox" is impenetrable. Even if that could be ensured, it cannot be done at a price and with remaining functionality that will allow the U.S. economy and customer service to function efficiently, swiftly, flexibly, at affordable prices and with continuing innovation. As institutions adjust to this new kind of crime, inevitably they will place more priority on security when trying to balance all of these other needs, but the Guidelines do not appear to consider any need except for security.

(7) **Part II,C, Containment and Control.** Part II, C (iii) of the Guidance includes among the measures to contain and control an incident, "ensuring that all known vulnerabilities in the financial institution's computer systems have been addressed." This requirement raises several questions, some of which are as follows:

(8) **A. How can a financial institution know "all" vulnerabilities** in a world in which systems are the subject of intentional criminal attacks limited only by the imagination and energy of the criminal, and a world in which all systems are potential targets.[8] Once the target of an attack is actually known, software publishers or others endeavor to publish notice of the possible attack,[9] but given the software subject matter and if the attacks are concerted, rapid or designed to attack even the cure, no one can "ensure" that "all" attacks can be addressed. This is complicated by the fact that no software application operates in isolation: each is affected by other applications, hardware and varying configurations and loads which cannot be envisioned or stated in advance by anyone.

(9) Software applications of the type needed to conduct modern business contain millions of lines of code and each application must work with many others. Thus, what may be a simple "patch" for one financial institution may be more complex for another[10] and no one can "ensure" that an attack cannot happen. Every application is fair game to a criminal or to someone who does not view themselves as a criminal but "simply" seeks to prove their prowess. Typically, no one approach will be automatically appropriate for every institution, and imposition of a blanket approach may have unintended consequences.

(10) **B. What is a "known" vulnerability?** A financial institution may "know" about a particular function but may reasonably believe that it is not a threat, is not material or may characterize the threat as less than critical to the institution given its particular circumstances based on information and risk balancing then available. For example, a recent report by Symantec, a software publisher of security technology, indicates that "99% of all events detected by Symantec during the first six months of 2003 were classified as non-severe and did not represent an immediate threat to the companies in the sample set. It is probable that this type of "noise" constitutes the vast majority of attacks detected by companies throughout the Internet, which explains why companies often experience such difficulty isolating "real threats" from the vast amounts of attack data."[11] These companies may "know" of the threat but in 99% of the cases that knowledge was not relevant. If an incident actually occurs, when was there a "known vulnerability?" By analogy, if a financial institution installs bullet proof glass on a drive-up teller's window knowing that the glass might not be effective against an uncommon bullet type or in circumstances not likely to occur, did the institution "know" of the vulnerability when it installed the

---

[8] See e.g., Symantec Internet Security Threat Report at 1 (9/03) (http://ses.symantec.com/PDF/SISTR_sept2003_all.pdf)(noting that some Microsoft applications are targets, that Linux may be targeted for future attacks, and that peer-to-peer systems are infection vectors).

[9] For an example of kinds of notices published by Microsoft, see http://www.microsoft.com/security.

[10] See e.g., FDIC guidance on patch programs, which guidance takes a more nuanced approach. Copy available at http://www.fdic.gov/news/news/financial/2003/FIL0343a.html.

[11] Id. at 9.

glass, when it became aware that such bullets or circumstances were actually being exploited by bank robbers, or at some other moment?

(11) It is also the case that there might not be time to act effectively or responsibly within the time assumed by the Guidance. A recent report indicates that malicious code is being used with increasing speed (64% of cyberattacks in the first half of 2003 targeted vulnerabilities less than a year old).[12] The W32.Blaster occurred only 26 days after the vulnerability it targeted was discovered.[13] The Guidance does not set deadlines. But it also does not make it clear that a response involving testing or law enforcement investigations will be allowed before notice must be given, including notice that could jeopardize the investigation or make it more difficult to locate the source of the problem (such as when a byproduct of notice to customers is direct or indirect notice to the criminal that discovery has occurred).

(12) Part III, "Standard for Providing Notice," does assume that an institution may both monitor and conduct an "appropriate investigation," but it may also create a Catch-22. The primary obligation is to notify affected customers "whenever it becomes aware of unauthorized access." The investigation is an exception to that rule and literally only applies if the institution can reasonably conclude that there is no real threat: if it cannot so conclude, the primary rule appears to apply, i.e., the institution should have notified the customer when it became "aware," a time before the investigation. Perhaps the wording could be revised to make it clear that an investigation is always allowed before notice is given, including involvement of law enforcement or similar officials and consideration of their recommendations.

(13) **Discrimination Against Electronic Commerce.** In the federal Electronic Signatures in Global and National Commerce Act Congress enabled an electronic U.S. economy. Whether E-Sign applies or is only used by analogy, 15 U.S.C. § 7004(b) preserves regulatory authority to issue regulation or guidance but also limits that authority: the issuance must be authorized by statute;[14] must be consistent with E-Sign § 101, which generally creates an equivalency between paper and electronic transactions; must not add requirements; and the agency must find that there is substantial justification for the guidance, that the electronic requirements are substantially equivalent to "paper" requirements, that the requirement will not impose unreasonable costs on the use of electronic records, and that it does not accord greater status to any particular technology for performing various functions, including storing electronic records.[15] Putting aside the legal question of whether the agencies must comply in these particular circumstances, the question is whether they should comply if only to avoid discrimination against e-commerce.

(14) The Guidance literally applies to all records, paper and electronic,[16] but it is primarily directed towards electronic records. For example, its containment and control measures require, depending upon facts and circumstances, the following measures for "computer intrusions:"

> (i) Shutting down applications or third party connections; (ii) reconfiguring firewalls in cases of unauthorized electronic intrusion; (iii) ensuring that all known vulnerabilities in the financial institution's computer systems have been addressed; (iv) changing computer access codes; (v) modifying physical access controls; and (vi) placing additional controls

---

[12] Symantec Internet Security Threat Report at 2 (9/03) (http://ses.symantec.com/PDF/SISTR_sept2003_all.pdf).
[13] Id.
[14] See Note 7 and 15 USC § 7004(b)(1)(A). It is not clear here whether the agencies are empowered to issue the Guidance.
[15] 15 USC § 7004(b)(2).
[16] "Customer information" is defined as including any "record" in "paper, electronic, or other form." Part I, Footnote 3.

on service provider arrangements.[17]

Assume a warehouse filled with labeled boxes containing sensitive paper records and a database system containing the same records. Each facility is secured: the warehouse has a 24-hour armed guards walking the perimeter, alarms and locked doors; the computer system has firewalls and requires access codes and so on. There is an incident indicating that the security of both systems has been breached for at least 48 hours: a guard discovers an open window, footprints of about 10 people, evidence of film debris and alarm tampering; the system administrator discovers penetration of the database by an unauthorized person. In each case, the entire warehouse or database, or critical parts, could have been accessed (or filmed). The Guidance does not provide an example of what the financial institution should do with respect to the warehouse and, indeed, taking all the equivalent actions could shut down the institution entirely if access to warehouse records is required by the institution or its service providers on a daily basis. What is the equivalent of the quoted text that must be done as to the warehouse? The fact that there is no ready answer illustrates that the actual focus of the Guidance is on electronic records. Given that, there is serious question whether the Guidance is authorized by E-Sign or equivalent public policy that should not discriminate against e-commerce.

(15) **Application.** Clarification that the Guidance is only intended to apply in contexts where regulators are the enforcement mechanism may be in order. Much of the language in the Guidance assumes enforcement by a regulator acting reasonably, i.e., a regulator who will make a reasonable assessment of whether an investigation was "appropriate," whether a conclusion of little likelihood of misuse was "reasonable," and whether control measures taken were appropriate given the "facts and circumstances."[18] Regulators know full well that there are really two victims in security attack situations: the customer whose information may have been accessed and the financial institution whose security was criminally attacked. Although both victims can try to prevent this kind of concerted crime, it would be curious public policy to further victimize the financial institution by subjecting it to customer suits or state legislation based on or paralleling the Guidance. The Guidance looks primarily to one victim, the customer. It does not include the protections for financial institutions that would typically be included in any law or doctrine allowing suit by private parties.

(16) We hope these comments have been helpful and thank you for your consideration of them.

Sincerely,

MICROSOFT CORPORATION

William Ashworth
By
William Ashworth, Policy Counsel

Susan Koeppen
By
Susan Koeppen, Senior Attorney

[17] Part I,C.
[18] Part II,C.